⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平3－185551

⑤Int. Cl.[5]	識別記号	庁内整理番号	㊸公開　平成3年(1991)8月13日
G 06 F 15/00	330 A	7218－5B	
1/14			
15/20	586 Z	7165－5B	
G 09 C 1/00		7343－5B	
		7459－5B	G 06 F 1/04　351 A

審査請求　未請求　請求項の数 16　（全11頁）

㊹発明の名称　デジタル時間認証装置

㉑特　願　平2－260322
㉒出　願　平2(1990)9月27日
優先権主張　㉜1989年10月13日㉝米国(US)㉛421,104

㉒発明者　アディソン・エム・フイツシヤー　アメリカ合衆国、フロリダ州、ネイプルズ　フオーテイーンス・アベニユ・サウス、60
㉑出願人　アディソン・エム・フイツシヤー　アメリカ合衆国、フロリダ州、ネイプルズ　フオーテイーンス・アベニユ・サウス、60
㉔代理人　弁理士　深見　久郎　外2名

明　細　書

1．発明の名称

デジタル時間認証装置

2．特許請求の範囲

（1）　デジタル時間認証装置であって、

コンポーネントを支持するためのプラットホーム手段と、

前記プラットホーム手段により支持され、時間を示すクロック信号を発生するためのクロック手段と、

前記プラットホーム手段により支持され、暗号キーを使用して前記クロック信号および入力値に関して動作しかつ認証タイムスタンプを発生するためのプロセッサ手段とを含む、装置。

（2）　前記プロセッサ手段に結合され、比較的予測不可能な出力値を発生するための乱数発生器手段をさらに含み、前記プロセッサ手段が前記予測不可能な出力値を使用する前記認証タイムスタンプを作成する、請求項1に記載の装置。

（3）　前記乱数発生器手段がノイズ発生ダイオードを含む、請求項2に記載の装置。

（4）　前記乱数発生器手段が前記プロセッサ手段により実行されるサブルーチンを発生する乱数を含む、請求項2に記載の装置。

（5）　前記クロック手段が複数のデジタルクロックを含む、請求項1に記載の装置。

（6）　前記複数のデジタルクロックの出力を受取るべく結合され、前記複数のデジタルクロックの出力の平均である時間出力信号を発生するための平均手段をさらに含む、請求項5に記載の装置。

（7）　前記複数のクロックの出力の間の差が予め定められたしきい値を超える場合エラー信号を発生するためのしきい値検知手段をさらに含む、請求項5に記載の装置。

（8）　前記装置を効果的に不正使用できないようにするための手段をさらに含む、請求項1に記載の装置。

（9）　前記クロック手段と前記プロセッサ手段が容易に不正変更され得ないように前記プラッ

トホーム手段上に前記クロック手段と前記プロセッサ手段とをカプセル化するための手段をさらに含む、請求項８に記載の装置。

（１０） 前記プロセッサ手段に結合されたスイッチ手段をさらに含み、前記プロセッサ手段が前記スイッチ手段の状態の変化に応答して前記装置が適当に動作することを妨げるための手段を含む、請求項８に記載の装置。

（１１） 前記プロセッサ手段が前記入力値および前記クロック信号について公衆キーデジタル署名動作を達成するための計算手段を含む、請求項１に記載の装置。

（１２） 前記プラットホーム手段上に配置されかつ前記プロセッサ手段に結合され、公衆キー・個人キーの対の秘密の個人キーを記憶するための記憶手段をさらに含む、請求項１に記載の装置。

（１３） 前記プラットホーム手段上に配置され前記プラットホーム手段上に配置されたコンポーネントに電力を供給するための電源手段をさらに含む、請求項１に記載の装置。

（１４） 前記入力値が少なくとも１つのデジタルメッセージを表わし、かつさらに前記プロセッサ手段に結合され前記入力値を受取りかつ前記プロセッサ手段へ前記入力値を与えるための入力手段を含み、それにより前記装置がタイムスタンプされるべきデジタルメッセージを受取りかつタイム・スタンプ認証デジタル文書を通信システムへ伝送するための前記通信システムに結合され得る、請求項１に記載の装置。

（１５） 前記プロセッサ手段が公衆キー・個人キーの対を発生するための手段を含む、請求項１に記載の装置。

（１６） 前記プロセッサ手段が認証初期化が完了したという表示を記憶するためのフラッグ手段を含む、請求項１に記載の装置。

３．発明の詳細な説明

この発明は総括的には電子的に転送されるデジタル文書をデジタルでタイムスタンプする装置および方法に関する。より特定的には、この発明は公衆キーの日付・時間認証設備としての役割を果たす方法と装置に関する。

発明の背景および要約

電子郵便システム、電子資金転送システム、電子文書転送システムその他の急成長により固定されていない通信チャネルで転送されるデータの保安についての心配が増大してきた。そのような固定されていないチャネルで通信されるメッセージのプライバシーおよび真正を確実にするために暗号システムが広く使用されている。

さて情報および文書がデジタル的に作成され、転送されかつ記憶されると、そのような情報および文書を真正認証しかつ認定するための新たな必要条件が存在する。

紙の媒体と違い、デジタルの原本は容易に変更され得る。さらに、化学物質および手書きの時間の経過ならびに作用が真正および時間の経過を推測するためのいくつかの手段を与える物理的に書かれた実例と異なり．．．デジタルの情報の時間の経過または真正を推測するための一応の（ｐｒｉｍａ　ｆａｃｉａ）方法は存在しない。

現在、公衆キーのアルゴリズムの到来によりデジタルの真正認証の手段が可能となった。これらシステムは、たとえば米国特許第４４５０８２９号により記載されるＲＳＡ暗号システム（ＲＳＡ Ｃｒｙｐｔｏｓｙｓｔｅｍ）等の簡単な使用によりもたらされるような、基本的な署名システムから、組合わされた署名の保護の相互ロックを可能にする、本件出願人の米国特許第４８６８８７７号により記載されるようなより複雑な承認システムまで様々である。

デジタル署名の場合、典型的には個人の資格は（彼の公衆キーを使用するための彼の承認）は固有に期間終了の日付で拘束されている。このような制限に関しては多くの理由が存在する。それらの１つはこのようなシステムではどれでも、（偶然にも）暴露された、またはその所有者が事前に承認を剥奪された公衆キーに対しての取消しの通知を受取りかつ保持することができる必要が存在するという事実に起因する。一般的には、このような取消しの通知は少なくとも資格の一応の期限

終了まですべての加入者により保持される必要がある。期限終了の日付が特定されていなければ、そのような通知は永遠に保持されなければならないであろう。

犯罪者が彼らの期限終了の日付を逃れようと希望すれば、彼はいくつかの場合においては、彼らのコンピュータ内のクロックを単純に戻してセットしたりかつ明らかに過去の時間に彼らの署名を行なうかもしれない。

また、特定の事象に関連する時間および／または日付が実際に正確であるということを確認することが有用でありまた時には決定的に重要である多くの情況（特にますます増大する量のビジネスが電子的に行なわれている今日ではそうである）が存在する。たとえば、発明の開示の文書の日付により発明者の発明における貴重な所有権の利益が守られるかまたはそのような利益を獲得しないかという違いが生じ得る。商取引においては、契約または受注に関するものとして報告された時間が実際に正確であるということを確認することは重要であるかもしれない。いずれの場合でも、使用者が日付をさかのぼって署名する可能性が存在すれば、使用者は時間的に誤って表わされた文書を作成する可能性がある。

このような問題を解決する１つの方法はすべての重要な文書に公平な第三者の「デジタル認証」サービスにより署名させかつタイムスタンプさせることである。そのような第三者を見つけることは困難かもしれない、または時期を得た対応でサービスを得ることは困難かもしれない。個々の使用者が、そのようなデジタル認証を容易に手に入れることは不可能かもしれない。その上、この方法では過ちが生じやすく、冗長でかつ隘路の原因になりやすく、かつまた潜在的に保安上の侵害をつくり出す可能性がある。

この発明は確実な方法で時間認証を達成しかつ、上記の「デジタル認証」アクセス能力の問題を取り除き、それによりいかなる個人または企業によっても使用することが容易な認証を行なうための装置および方法に向けられる。その上、この発明はだれでもその認証を確証しかつその認証タイムスタンプに頼ることが容易なように時間認証を達成する。装置は経済的であり、かついかなる外部のサービスの使用も顧みず局部的に使用が可能である。

この発明はそれによりどのようなデジタル情報でも認証において述べられた明白な時間において存在したものとして効果的に認証され得る。このことはどのようなごまかしによる電子的な日付の後戻しの可能性をも除去する。

この発明の時間認証装置および方法は第三者による干渉が最小限で信頼できるタイムスタンプを得るために公衆キーの暗号動作を達成する、確実な、マイクロプロセッサベースのハードウェアのプラットホームを使用する。ハードウェアのプラットホームは装置のタイムスタンプ機構が破壊されたりまたは変更されたりすることができないように確実な態様でカプセル化される。

ハードウェアのプラットホームは少なくとも１つのデジタルクロックと公衆・個人キーの対の個人の半分を記録する、安定した、安全な記憶装置を含む。デジタルクロックと記憶装置の双方に連結されるのは確実でかつ不正変更できない態様で公衆キー署名動作を達成するデータ処理装置である。処理装置だけが安全な記憶装置およびその関連する個人キーへのアクセスを有する。

ハードウェアのプラットホームはまたデジタル的に署名されかつタイムスタンプされるべきデジタルメッセージを受取る入力・出力手段を含む。入力・出力手段は装置により発生する結果として得られるタイムスタンプされた署名を文書の提示者に返却もしくはデジタルタイムスタンプを記憶または何かほかの適切な手段でそれを処分し得る。ハードウェアのプラットホームはまた電力源（たとえば、オンボードバッテリー）を含み、装置の使用寿命の間を通して連続的に装置のデジタルクロックの精度および記憶されたデータの保全を確実にする。

この発明のこれらおよび他の目的ならびに利点は添付の図面に関連して考慮される現在の好ま

しい例示的実施例の以下の詳細な記載を読むことでよりよく認識されるであろう。

図面の詳細な説明

第１図はこの発明の例示的実施例に従う日付・時間認証装置１のブロック図である。簡単に述べれば、装置１はクロックモジュール４を含み、それはプロセッサ６に結合される。プロセッサ６はまた記憶装置８および乱数発生器１０に結合される。これらコンポーネントおよびオンボード電力源１２の各々がプリント回路またはコンピュータ板２上に装着される。回路板２およびその上に装着されたコンポーネントは記憶装置８の内部が外部からのアクセスまたは観察が不可能なようにかつクロックモジュール４内のデジタルクロック（又は複数のクロック）が簡単に不正使用されたり変更されたりできないような確実な態様でパッケージされる。

装置１が効果的に不正使用されないようにするために使用され得る１つの方策は回路板上のコンポーネントの上にエポキシを配置しそれによりコンポーネントのピンが破壊を伴わなければ探られたりまたは不正変更され得ないようにすることである。コンポーネント自体が物理的な干渉に対して感応的に設計されてもよく、したがってたとえばプロセッサ６内の一般レジスタに関連する数値が物理的干渉に応答して修正される。この点に関してはプロセッサ６はそれをケースに入れるエポキシ内に埋没するスイッチ（図示されていない）に連結された１つまたは２つ以上のその入力ピンを有し得る。そのようなスイッチは干渉に応答して閉じる（または開く）であろうし、たとえば、そのような入力ピンの状態の変化に応答して、プロセッサ入力ピン上にはっきりした信号レベルを発生する。プロセッサ６はそれからたとえば、プロセッサレジスタに記憶された個人キーの値の抹消を含む、予め定められた値を順に、修正または抹消し、もしくはエラールーチンに分岐し、それにより公衆キーの日付・時間認証装置が適当に動作することまたは個人キーの値が発見されることを防ぐ。

より詳細に第１図に注目すると、上記のとおり、日付・時間認証装置１内にクロックモジュール４が埋め込まれる。クロックモジュール４はたとえば、品番ＭＭ５８２７ＢＮ等の商業的に入手可能なデジタルクロックを含む。クロックモジュール４はその出力線３および５上にタイムスタンプ値Ｖ１を発生する。タイムスタンプ値Ｖ１は上に記載されるとおり単一のデジタルクロックの出力でもよい。代替的には、値Ｖ１は２つまたは３つ以上のデジタルクロックの出力の平均でよい。またそれはクロックが故障していると思われるときにはエラー信号（図示されていない）を発生する。

第５図はたとえば２０、２２等の多重デジタルクロックを有する例示的なクロックモジュールのブロック図を示す。デジタルクロック２０および２２の出力はクロック２０および２２のタイムスタンプ信号を平均する平均値発生回路２３に結合されかつクロックモジュールタイムスタンプ値Ｖ１として出力線３および５上に平均時間を出力する。

デジタルクロック２０および２２の出力は、たとえば、クロック２０と２２のデジタル出力の間の差を示す信号を発生する減算器２４に連結される。クロック２０と２２の出力の差はそれからしきい値検知器２６に連結される。もし万が一、クロック信号の差が１日当たり数ミリ秒より大きい差に相当する予め定められたしきい値を超えると、しきい値検知器２６がエラー信号を発生し、それは出力線３を介してプロセッサモジュール６に連結される。プロセッサモジュール６はエラー信号をデコードしかつ装置１を不能化しかつ個人キーを抹消するエラールーチンに入る。

多重デジタルクロック２０および２２の使用が望ましいのは正確なタイムスタンプを発生するためには日付・時間認証装置１に依存するからである。単一のデジタルクロックは（時間がたてば）不完全な態様で動作し始める可能性があるので、上に述べられるとおり、しきい値検知器に連結された２つ（またはそれ以上）のデジタルクロックを使用することによりクロックモジュールが正確

なタイムスタンプを発生する可能性を実質的に強化する。加えて、多重デジタルクロックを使用することでだれかがクロックモジュールを不正使用していることを検知する機構がもたらされる。この点に関して、デジタルクロックの１つの出力が妨げられると、しきい値検知器２６を使用することで、エラー信号を発生させることが可能と考えられかつ装置１はその後に不能化されるであろう。減算器は、「クロック」モジュールで示されているが、実際にはプロセッサ（６）により達成されてもよい。チェックは文書が提出されたときのみに達成されることが可能かまたは好ましくは連続的に実行されることが可能であろう。

第１図に戻ると、プロセッサモジュール６はたとえば、インテル－２８６（Ｉｎｔｅｌ－２８６）マイクロプロセッサ等の商業的に入手可能なマイクロプロセッサでよい。プロセッサ６は確実でかつ不正使用ができない態様で公衆署名動作を達成または組合わせるのに十分な独立した計算出力を有するものならどのようなマイクロプロセッサでもよい。

プロセッサモジュール６に結合されているのは記憶装置８でその内部に公衆・個人キーの対のうちの秘密の個人キーが記憶される。重要なことは記憶装置８の内部のみがプロセッサモジュール６へアクセス可能である点である。記憶装置８は使用者が記憶装置の内容すなわち、個人キーを決定することができないような安定した、確実な記憶装置でなければならない。記憶装置８は好ましくはプロセッサモジュール６のプログラムメモリとしてもまた動作し得るリードオンリーメモリ（ＲＯＭ）である。記憶装置８はプロセッサモジュール６内で実施され得る。不正使用の試みに関するいかなる検知によってもこの値は破壊されるはずである。

日付・時間認証装置認証１もまた電力源１２を含み、それは装置１が孤立的に動作しかつ装置が装備されていないとき（たとえば運搬の間）、第１図に示されるコンポーネントへ電力を与える比較的長寿命のオンボードバッテリでよい。代替的には、さらに以下に説明するように、装置１がたとえば関連するコンピュータシステムと関連して動作している場合、その時は装置１は外部から電力を与えられかつ電力源１２が、停電の場合にはバッテリバックアップとしての役割を果たすであろう。それはまたそれが初期化されるとき（工場で）と使用者が外部の電力源へプラグを入れるときとの間、システムを「活性」状態に保つ役割を果たすはずである。

例示的な日付・時間認証装置１はまたプロセッサモジュール６に連結された乱数発生器１０を含む。乱数発生器１０はプロセッサモジュール６による公衆キーの署名動作において使用される乱数値Ｖ３を導入する。乱数発生器１０はさらにオン動作されるランダム入力を導入することにより公衆キーの署名プロセスへ暗号の強度のさらなる程度を導入する。各署名にこの乱数値を含めることにより、署名システムを解く上である予知しない利点を対抗者に与えるかもしれない特定の値が対抗者により供給され得ない。乱数発生器１０は、たとえば乱数値Ｖ３を発生するために使用される予測できない出力を発生するノイズダイオードから構成され得る。このようなランダム値発生器は商業的に入手可能でかつ、たとえば品番１Ｎ７５１等を含み得る。ランダム値発生器１０は代替的にはたとえば、値Ｖ３を発生するためのアルゴリズム（それについては多くの周知のものが存在する）を発生するいかなる妥当なランダム値または擬似ランダム値を使用するプロセッサモジュール６によっても実行されるサブルーチンにより実現され得る。ランダム発生器は実際には任意のものでありかつアルゴリズムの理論的強度を増大する役割を果たすのみである。

日付・時間認証装置１が動作する態様を記述する前に、装置の入力、出力および装置１が典型的に動作するシステムが第２図との関連において記載される。装置１は典型的には処理システム１４に結合されるものとして考慮され、そのシステムはたとえば、ＩＢＭ－ＰＣまたは同様のものでよい。回路板２は物理的にＰＣに挿入されそれによ

りＰＣのポートの１つに結合されることになる。この点に関しては、回路板２はたとえば、表示インタフェースカードと同様の態様でＰＣポートに結合されるであろう。処理システム１４は順にたとえば、電話リンクなどを介する電気通信システムに結合され、それにより伝送されたファイル、メッセージまたは文書をデジタル的に受取ることが可能である。

ＰＣはたとえば、署名されるべき電子文書を受取るとその出力線１５を介して認証されるべきデジタルビットストリームＶ２を入力する。その後、認証タイムスタンプを含む認証証明がセットされたパケットが初めに署名されるべき電子文書を送信する側に返えされる。処理システム１４はもちろん、ＰＣである必要はなく、むしろより大型の主フレームのコンピュータすなわち電気通信システムその他を含む装置のネットワークでもよい。

署名されかつ時間認証されるべき入力値Ｖ２はいかなるデジタル値でもよく、たとえば実際では購入の注文、契約書、文書の創作者になり代わって特定の動作を達成するための授権、または予め定められた時間までにその文書が存在したことを証明することが重要であるいかなる他の形式の文書をも表わし得るデジタル文書を含んでよい。日付・時間認証装置１は文書に示された時間の後の時間における時点でその文書が作成されなかったということを証明するべく使用され得る認証タイムスタンプを発生する。入力Ｖ２はまたそれ自体がさらにもう１つのデジタル値の使用者のデジタル署名となり得る。装置はまた入力Ｖ２の寄せ集めをつくり出し、かつその寄せ集めを入力Ｖ２全体というよりはむしろその署名に埋め込む。

この発明の例示的実施例では、認証証明がセットされたパケットは日付・時間認証されるべき元のデジタル文章を伝送する側へ返される４つの値を含む。この点では、第２図に示されるように、認証されるべきデジタル文書または入力値Ｖ２が文書の創作者へ返される。付加的には、クロックモジュール４の時間出力である、タイムスタンプ値Ｖ１が文書の創作者へ返されかつ認証されたタイムスタンプＳもまた返される。タイムスタンプ値Ｖ１はクロックモジュール４が発生することのできる最も正確な時間を反映する。タイムスタンプＶ１は、すでに述べられたとおり、モジュール４における多重クロックが完全な同期化の状態にある予め定められたしきい値の範囲内による場合にのみ発生される。クロックモジュール４におけるデジタルクロックの各々の出力が、所望なら、それぞれ伝送され得ることに留意されたい。いくつかの場合には、ＲＳＡを含むいくつかの署名システムで、「Ｓ」値を保持することのみが可能になるかもしれない、というのはＶ１はそこから引抜かれ得るからである。他方、Ｖ１同様Ｖ３を保持することが必要になるかもしれない。

プロセッサ６により達成される動作の一般的なシーケンスが第６図のフローチャートに示される。簡単に言えば、プロセッサ６は値Ｖ１、Ｖ２およびＶ３の各々ならびに記憶装置８内にある秘密のキーとをたとえば、その動作ＲＡＭ（図示されていない）内に入力しかつ一時的に記憶する。プロセッサ６は入力値Ｖ２を得るが、それは入力を受取る線１５を介して認証されるべき文書であり、かつこの値を線３を介して受取られるタイムスタンプＶ１および公衆・キー暗号署名動作を使用してモジュール１０より発生されるランダム値と組合わせる。この点では、値Ｖ１、Ｖ２およびＶ３の組合わせが記憶装置８内に記憶される秘密の個人キーを使用するモジュール６により処理される。署名プロセスはたとえば、米国特許第４４０５８２９号に教示されるＲＳＡデジタル署名技術を使用して達成され得る。

例示目的のためにのみ、第６図に示されるように、５１２ビット（６４バイト）のＲＳＡ署名が使用されると仮定すると、Ｖ２は入力でありかつそれはまたはその寄せ集めが認証されるべきＶ２である入力文書を表わす６４バイトのデータのより低いオーダーの１６バイトとして一時的に記憶される（１００）。署名システムと関連して使用され得る多くの周知のハッシング方法が存在する。６４バイトの値の他の８バイトは線３を介する入

力でありかつ一時的に記憶される（１０２）クロックモジュール４の出力であるＶ１を記憶するために使用される。値における残りの４０バイトは乱数発生器１０から受取られる入力から構成されるランダムビットからなるかもしれない（１０４）。この６４バイトの数字はそれからたとえば米国特許第４４０５８２９号の教示に従い記憶装置８に記憶されたＲＳＡ個人キーで指数化される（１０６）。これはデジタル署名を発生する。６４バイトのデータを記憶された個人キーで処理した後、出力署名値が記憶され（１０８）かつ認証されたタイムスタンプＳとして第２図に示されるものを出力する（１１０）。入力Ｖ２とタイムスタンプが署名に備えて組合わされることが可能な多くの方法が存在する。

認証されたタイムスタンプ証明のセット（Ｖ２、Ｖ１、Ｓ、Ｃ）に含まれる最終の値は、その文書が日付・時間に認証されている側へ伝送されるが、これは製造業者の証明Ｃである。第２図に戻ると、そこで言及される製造業者とは日付・時間認証装置１の製造業者である。製造業者の証明Ｃはその内部に装置の個人キーに関連する公衆キー１６と製造業者の公衆キー１７とを実現しているであろうし、かつ信頼のおける製造者による装置の公衆キーのデジタル署名を含むであろう。

可能な多重レベルのデジタル証明および例示的デジタル証明の本質に関するさらなる詳細が１９８９年９月１９日に発行された本件出願人の米国特許第４８６８８７７号に見られかつそれは「強化されたデジタル証明を有する公衆キー・署名暗号システム」と題され、ここに引用により援用される。本件出願人の特許に詳細に記載されるように、装置の公衆キーは所望されれば、その作成者の承認を識別するような態様で証明され得る。証明のプロセスはこの新しい公衆キーに信頼のおける製造者の個人キーで署名しかつ所望されれば表現的に署名者によって認められた承認を示すステップを含む（すなわち承認とは信頼のおける時間認証である）。その署名に使用される製造者の公衆キーがよく認識されているものであるため、そのような信頼が単純に暗に含まれ得る。この点では、信頼のおける授権者（すなわち製造者）は十分公表された公衆キーを有するものとして考慮され、そのキーは既知でありかつその装置のすべての潜在的使用者により受入れられる。そのような製造者は単にその個人キーの部分を使用して装置の新しく作成された公衆キーにサインする。代替的には本件出願人の特許に記載されるように、信頼のおける時間認証者として委任された授権者は証明の階級により制御されるかもしれないし、または製造者の署名が単一の製造者の代表者またはいかなる単一の側によっての不正の危険をも減じるために１人または２人以上の証人により必要とされる共同署名を示すかもしれない。そのような場合には、装置の証明はこれら署名のすべてに関する情報を含む必要があるであろう。代替的には、米国特許第４４０５８２９号は製造業者の公衆キーの広範囲な受容および認識により単純に正当であると確認されるであろう単純な、１つのレベルの証明を発行するために直接的に適用され得る。

実際には、末端の使用者は装置１とともに装置に埋め込まれた秘密の個人キーに対応する公衆キーの写（フロッピーディスクで）と、この公衆キーに関する製造業者の証明と、装置１へいかなる入力をも与えるおよび装置１から対応する出力を伝達するために使用され得るプログラムとを併せて受取る。

タイムスタンプされ認証された署名Ｓ（Ｖ１、Ｖ２およびＣといったアイテムとともに）はそれからどのような物件であれ署名されたものが特定の瞬間に存在したこと（および特定の署名装置１の付近に存在したこと）を示す認証記録としての役割を果たす。一般的には、装置の出力された署名およびタイムスタンプ値Ｖ１は装置の関連する公衆キーおよび装置の公衆キーに関する製造業者の証明、ならびに製造業者の公衆キー（複数）により伴われ、それによりこれらのすべてがともに認証のための証明のセットとしての働きをするであろう。認証されたタイムスタンプはそれから伝送されおよび／またはその物件が特定の瞬間に存

在したという後々の証明のためにその物件とともに記憶され得る。認証される物件そのものが実際に、ある第３の物件（たとえば文書、購入注文書、その他）の何かほかの側によるデジタル署名である、特別な場合にはそのような署名の認証が本質的に署名する側がその特定の時間にまたはその以前に前記署名を作成したことを保証することに留意されたい。これは従来の認証公衆サービスにより達成される標準的機能に大変はっきり類似するものを提供する。

装置１が装填される態様は第３図に示されるフロー図により例示される。装置１が製造プロセスの間に最初に装填されるであろうことが考慮される。装填は製造業者の工場で装置１をその入力ポート１５（第２図参照）を経由して装填処理装置（図示されていない）へ連結することにより行なわれ得る。

第３図に示されるフロー図により示されるとおり、装置１は電力を与えられると（３０）直ちに初期化モードルーチン（３２）へ分岐する。初期化モードでは、装置１はクロックモジュール４が最初にセットされる（３２）装填状態に入る。クロックモジュール４はデジタルクロックを正確に初期化するためおよび動作を始めるためにそれらを開始するために世界的に認められた標準時間に基づいてセットされる。その後、プロセッサモジュール６はランダム値を使用する公衆キー・個人キーの対を内部で発生し、それはＲＳＡ公衆キー暗号（米国特許第４４０５８２９号または第４８６８８７７号参照）の教示に記載されたようなどのような公衆キー署名方法とも両立する態様でプロセッサ６により発生される（または装置の初期化の間に製造業者から受取られる）。その後、個人キーの部分は記憶装置８に装填される（３８）。個人キーの部分が記憶された後、装置の初期化が完了したことによりプロセッサ６が再び初期化され得ないことを確実にすることを示す「初期化フラッグ」がセットされる（３９）。

ステップ４０に示されるように、プロセッサモジュール６はそれからそれがプロセッサ装置初期化へのステップ３６で発生した公衆キーを伝送する。しかしながら、公衆・個人キーの対のうち個人のキーの部分は初期化プロセッサに伝送されないので初期化プロセッサでさえ秘密の個人キーには気がつかないことに留意されたい。その後、デジタル署名動作は伝送された公衆キー（４２）に関して信頼できる権威者、たとえば製造業者の個人キーを使用して達成される。初期化プロセッサは装置１のためのデジタル証明を発生するための署名動作（４２）を達成し得る。このように、製造業者は発生された装置の公衆キーに署名しかつその動作において、装置に関するデジタル証明を作成することにより（それは装置自体に記憶されてもよいしまたは装置から分離されたフロッピーディスクに記憶されてもよい）、時間・日付認証装置５が本物でありかつ信頼できるものであるということを確証する。この点に関しては、署名プロセスは署名する側がクロックが正確な時間に初期化された（４４）ことを確証したことを示す。さらに、装置のための証明に関連して製造業者の公衆キーが日付・タイムスタンプが真正であることを保証するための日付時間認証書類を受取る側により使用される。

所望されれば、公衆・個人キーの対はプロセッサモジュール６により発生されるよりもむしろ、初期化プロセッサにより発生されてもよい。この態様では、プロセッサモジュール６はその独自の公衆・個人キーの対を発生する能力を有する必要がないので、従ってプログラムの記憶に関しての節約となる。このように、装置１を初期化するための代替的な方法は第３図で示されるステップ３４において使用されるようなクロック値を初期化することであるが、プロセッサモジュール６に公衆・個人キーの対を発生させるよりはむしろ、このような対は初期化プロセッサにより装填されるであろう。初期化プロセッサはそこでそれが発生された直後にキーの対の個人の部分のその写を抹消するであろう。その後、初期化プロセスが第３図との関連において既に述べられたように進行するであろう。

日付・時間認証文書の受手は、電子的に文書を受取りかつ記憶した後そこで第４図に示されるフロー図に従いタイムスタンプを確証するであろう。そのようにタイムスタンプを確証することにより、使用者はその文書が示された日付および時間より前に作成されたことを証明することができる。受取られた文書上のデジタルのタイムスタンプは認証された入力値Ｖ２（５０）、タイムスタンプＶ１（５２）、認証されたタイムスタンプＳ（５４）および製造業者の証明Ｃ（６６、６８、７０）を含む。認証されたタイムスタンプＳ（５４）はその内部に第２図および第６図との関連において上記に記載されたような値Ｖ１、Ｖ２およびＶ３を埋め込んでいることに留意されたい。製造業者の証明Ｃおよび認証されたタイムスタンプＳは公衆キーの動作（５６）を介して処理されそれにより結果として得られる１６バイトの値Ｘ２、８バイトの値Ｘ１および４０バイトのランダム値Ｘ３が得られる。値Ｘ１、Ｘ２およびＸ３は、タイムスタンプが適当に認証されれば値Ｖ１、Ｖ２およびＶ３（それらは第２図との関連において上記に記載されている）に等しくなるはずである。種々の値を確証するために示されたそのステップがまさにＲＳＡのアルゴリズムに適する。他の公衆キーのアルゴリズムのためにはもう１つのシーケンスのステップ必要かもしれない。いくつかの公衆キーのシステムもまた「ランダム」値Ｖ３を知る必要があるであろうことに注目されたい。

Ｘ１はそこでブロック５８で示されるようなＶ１と比較されかつ結果が等しくなければ、そこでタイムスタンプは拒絶されるはずである。Ｘ１の結果がブロック５８で決定されるようなＶ１に等しければ、Ｘ２と認証されたＶ２であった入力値との間でブロック６０において比較が行なわれかつ結果が等しくなければタイムスタンプは拒絶される（６４）。

ブロック６０における比較の結果がＸ２がＶ２に等しいということを示せば、そこで入力値が、Ｖ１により示される時間に先立って意図的に作成されたということを決定するための基準の１つが満たされる。所望されれば、ランダム値Ｘ３は発生されたランダム値Ｖ３と比較され得るが、簡素化の目的でそのような比較は第４図では示されないことに留意されたい。

装置の公衆キーのチェックがまた第４図で行なわれる。この点に関しては、製造業者の証明から、製造業者により作成された、装置の公衆キー（７０）の署名および製造業者の信頼のおける公衆キー（６８）が公衆キーの動作（７２）を経由して処理される。公衆キーの動作の出力は装置（６６）に関する公衆キーを確証するはずである。装置の公衆キーと公衆キー動作（７４）の出力を比較する比較がなされる。ブロック７４で示されるようにマッチが存在しなければそこでタイムスタンプは拒絶されるというのは認証を達成した公衆キーが信頼に足るものとして認識されていないからである（８０）。ブロック７４および７６でのチェックがマッチが存在するということを示せば、そこで、その公衆キーが製造業者により作成された装置にまさに属するものであったということが確証される。その装置が製造業者により作成されかつタイムスタンプが装置の公衆キーにより作成されたものであるということが確かめられれば、そこで使用者はその文書がタイムスタンプＶ１により示される時間・日付に先立って作成されたものである（８２）ということを受入れることができる。

この発明は現在最も実際的でかつ好ましい実施例として考慮され得るものとの関連において記載されてきたが、この発明が開示された実施例に制限されるものではなく、先行の請求項の精神および範囲に含まれる種々の修正および等価な調節を網羅するものとして意図されることを理解されたい。

４．図面の簡単な説明

第１図はこの発明の例示的な実施例に従う公衆キー日付・時間認証装置のブロック図である。

第２図はタイムスタンプがどのように作成されるかを示す文書の入力および種々の出力に関して第１図の装置を示すブロック図である。

第３図は第１図の装置を装填しかつ初期化する

ための例示的方法を示すフロー図である。

第４図はタイムスタンプがどのように確証されるかを示すフロー図である。

第５図は例示的なデジタルクロックモジュールを示すブロック図である。

第６図は公衆キー署名動作を達成する上で第１図における装置により達成される動作のシーケンスを包括的に示すフロー図である。

図において、１は装置、２は回路板、４はクロックモジュール、６はプロセッサ、８は記憶装置、１０は乱数発生器、１２は出力源、２０はデジタルクロック、２２はデジタルクロック、２３は平均値発生器、２４は減算器、２６はしきい値検知器である。

特許出願人　アディソン・エム・フィッシャー

代　理　人　弁理士　深　見　久　郎

（ほか２名）

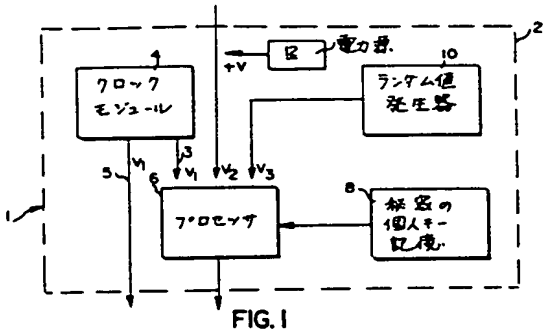
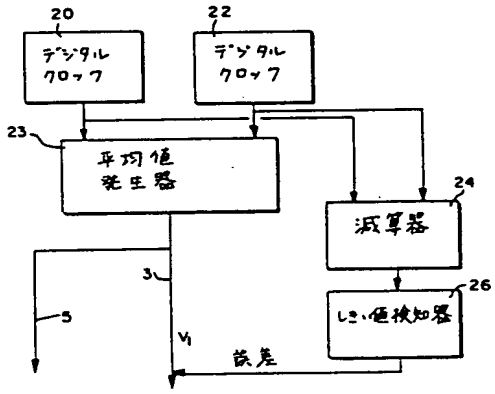


FIG. 1

FIG. 5



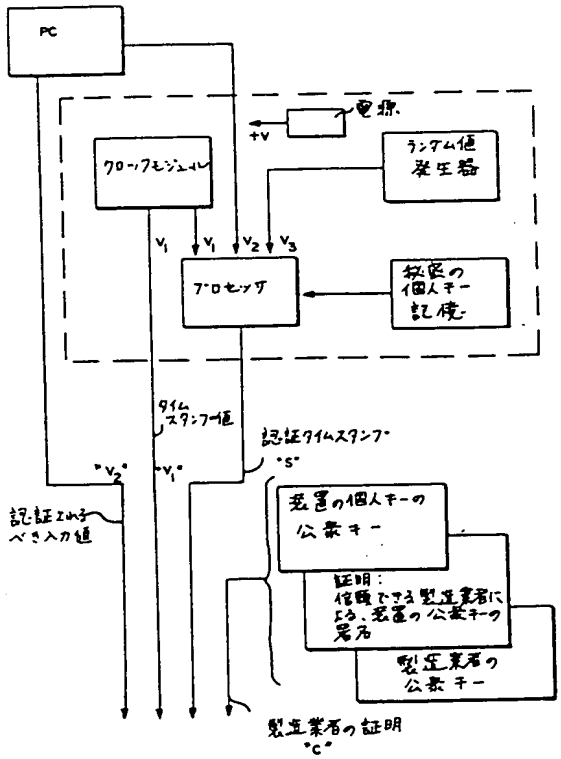


FIG. 2

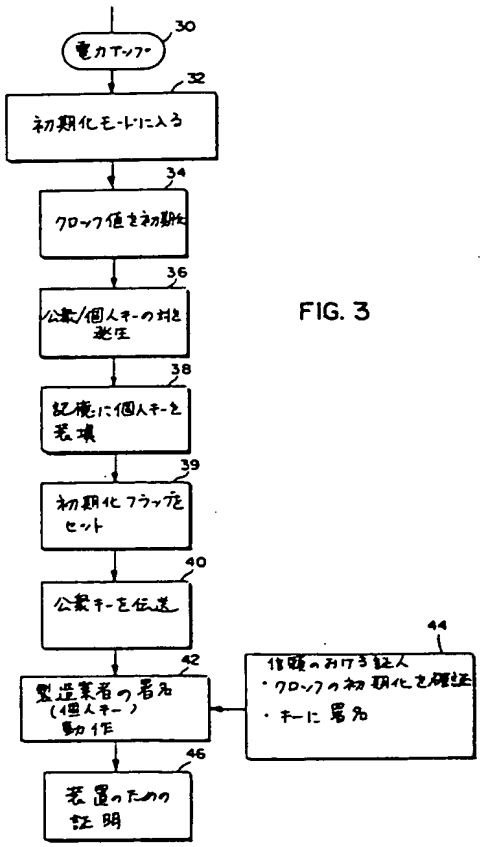


FIG. 3

図面の浄書

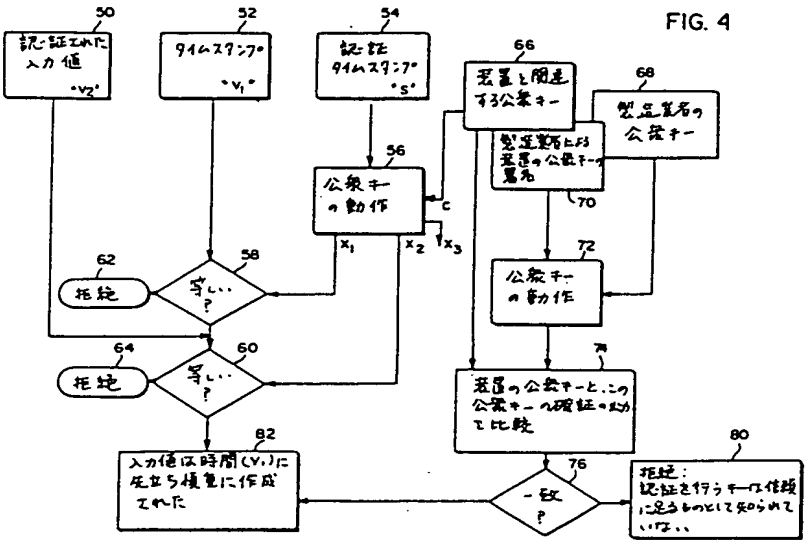


FIG. 4

図面の浄書

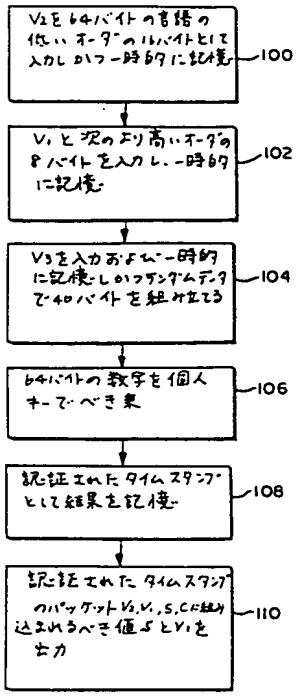


FIG. 6

手 続 補 正 書 (方式)

適

平成3年1月24日

特許庁長官殿

1. 事件の表示

平成2年特許願第260322号

2. 発明の名称

デジタル時間認証装置

3. 補正をする者

事件との関係 特許出願人

氏 名 アディソン・エム・フィッシャー

4. 代 理 人

住 所 大阪市北区南森町2丁目1番29号 住友銀行南森町ビル

電話 大阪(06)361-2021(代)

氏 名 弁理士(6474) 深 見 久 郎

5. 補正命令の日付

平成3年1月22日

特許庁

6. 補正の対象

図面の第4図および第6図、委任状および訳文

7. 補正の内容

別紙の通り

以上